Keeping Your Computer Secure

John Steele

Outline of presentation

- Talk based on Windows
  - Principles also apply to MAC and Linux computers
- Windows security model – how can it protect you
- How to work with Windows security
  - What to do right
  - What not to do
    - How to put it right if you have done it incorrectly
- Security associated with use of external services
  - Virtual Private Networks – Risks and Benefits
  - Email – differences between IMAP vs POP3
  - Cloud storage
  - Router configuration

Basic network security

- At home we have a Router that connects us to an Internet Service Provider
  - A Router allows outbound connections to a server somewhere in the Internet
  - A Router (should) prevent any inbound connection from reaching any device on your local network
- Other devices on your home network are free to make outbound connections to any other device on your local network
  - Your router MAY be configurable to allow inbound connection from the Internet to be made under certain circumstances – potentially VERY risky
    - PlusNet DO allow these inbound connection under certain conditions with their current router and the router needs to be configured to block it
    - A good AV product will also act as a filter to block connections to specific devices (but printers, TVs, other smart devices can also be exploited.
    - Windows firewall should also block inbound connections fom outside the local network

Firewalls

- A firewall is a function that monitors network traffic and attempts to block unexpected network packets whether these come from inside the local network or from outside
  - Outside attacks should be blocked by the router but there is no harm in having both your router and four firewall defending you!
- The Windows firewall is now very effective and usually configuration happens during program installation
- Many AntiVirus packages have their own firewall or control the settings of the Windows firewall
- To explain how this is all possible would require a whole new session!

Windows security model

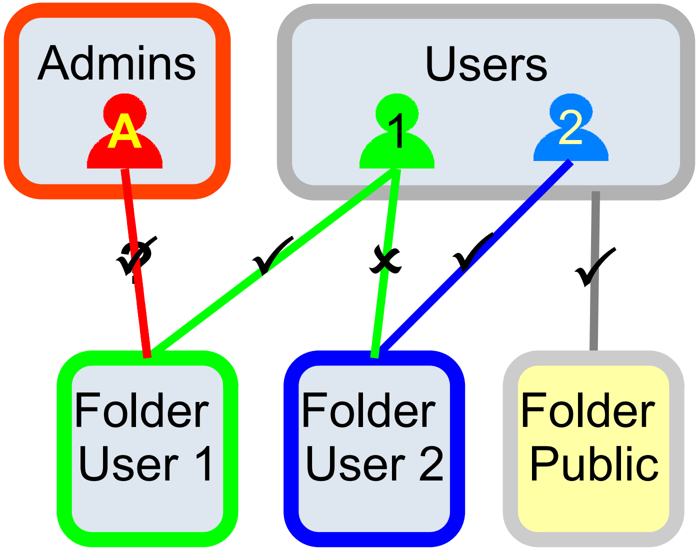
- Some basics:
  - All of Windows security is based on an authenticated user
  - Each user has a Windows account with an associated password
  - Each user is a member of one of more Groups. The groups, in a standard installation, will be a member of either the
    - User Group
    - Administrator Group

Windows local vs online account

- Microsoft are increasing their efforts to make you have an on-line account rather than a simple Local Account
  - This can help if you want to access your settings from different computers
  - The downside is less privacy
  - You always share a password between your Microsoft email and your computer
  - Your email account password should be strong but your local password need not be as strong
- You do NOT NEED a Microsoft account to access your own computer - I do NOT use one
  - You CAN still use the shared calendar and One Drive (and I do) and the Microsoft Store
  - A more detailed comparison can be found here https://www.lifewire.com/local-vs-microsoft-accounts-in-windows-3507003
- It can be a challenge however to avoid linking a Microsoft account to your local account when you first set up your computer
  - The best trick is to avoid connecting to the Internet initially until you have created your local accounts

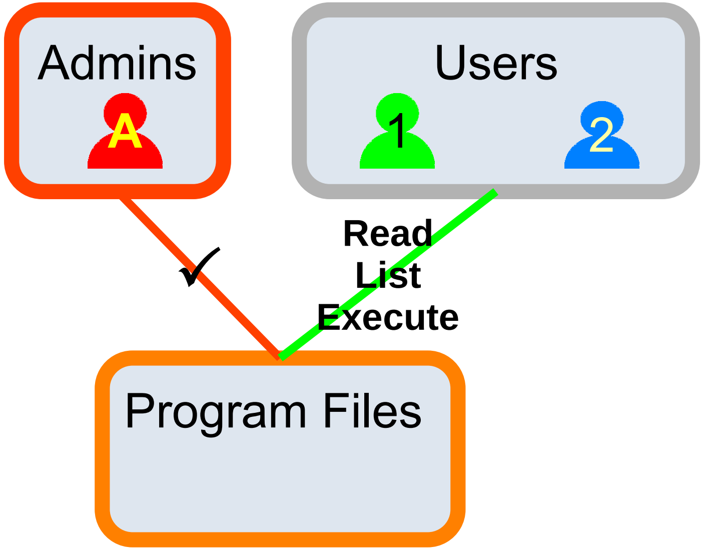
Permissions – User folders

- Access to user data is controlled by Permissions
  - User Permissions are inherited from Groups
- Users are created by Admins [A]
  - Two users are shown here [1] and [2]
  - Each has their own folder
  - There is also Public folder accessible to all
- [1] and [2] can create/read/write/delete documents in their own space and to the Public Folder
- [1] has NO ACCESS to data in [2] Folder
  - (unless explicitly granted access by [2])
- [A] also cannot initially access
  - **but can grant themself full read/write/delete access without reference to the owner**



Access to Program files

- Windows stores programs (Executables) in one of two special folders
  - Program Files
  - Program Files (x86)
- **Administrators have full access to these folders**
- User can
  - Read/List the contents
  - Execute (Run) programs
- **Users cannot write to this folder!**



Windows Installation

- Windows 10 is a VERY secure Operating System
  - Home users have EXACTLY the same basic security features available to them as any corporate systems
  - IF and only IF, it is installed and used correctly
- Microsoft has a standard method for manufacturers to prepare a system for easy installation by a user which has all of the manufacturer’s specific options pre-installed
  - e.g. device drivers to match the hardware, and any software that they choose to supply with their computer
- ALL manufacturers that I am aware of use this process
  - But I have not yet seen a manufacturer tell you how to do this properly!

What if you have not done this – simple steps!

- If you have inadvertently created your main account as Administrator It is relatively easy to correct the situation
- See the following links which give a number of ways to do this
  - https://www.howtogeek.com/226540/how-to-create-a-new-local-user-account-in-windows-10/
  - https://helpdeskgeek.com/windows-10/how-to-change-the-administrator-on-windows-10/
- The club web site guide on this topic has been updated to make the steps clearer
  - https://gxcc.org.uk/gxcc-docs/2021-06-GXCC-Windows-two-accounts.pdf

Protection against malware

- Running as using a Standard User rather than Administrator account provides better protection that any Antivirus product
  - I have seen a report that over 80% of malware attacks would be prevented by using a Standard User account even without any AV product
- Antivirus software still has a place however as an EXTRA defence
  - Windows Defender is now very good – is the default in Windows if no product installed
  - Free AV products are better e.g. Avast! or AVG (now same product)
  - Paid for versions MAY provide more immediate support but are NOT necessarily better
    - They can provide additional “benefits” e.g. Virtual Private Networks (see later!)
  - Kaspersky is known to be good, but if you are dealing with nationally sensitive material be aware that they share an office building with the Russian equivalent to GCHQ!
    - It is widely believed that American secret data has been leaked via this route (by someone breaking rules though)

Virtual Private networks - VPN

- VPNs are often touted as the answer to all your security issues
  - BEWARE – this is NOT true
- A VPN provides a secure “tunnel” between your computer and another server
  - The remote server can be located elsewhere in the world
  - It launches your Internet request from that server and not yours
  - It hides your IP address from the site you are connecting to

VPN – the downside

- A VPN and particularly the “free” ones
  - Can monitor your traffic and pass information to third parties
    - You may find their privacy notice (if they have one) may give them this right
    - Could “break” a secure SSL session (HTTPS) and intercept private data
      - Data would be unencrypted in their servers and scanned before it is re-encoded into SSL
      - “Man in the middle” attack
    - If outside EU or UK they do NOT have to comply with GDPR
  - Are providing simultaneous service to thousands of concurrent users
    - Are not immune to software issues and could “leak” data to other parties

VPN – When are they useful

- If you are using a company owned and managed computer away from a company site a VPN is ESSENTIAL
  - The VPN is established between a company owned and managed local computer and a company owned and managed VPN termination giving access to corporate resources
- If you are using your own computer in a VERY INSECURE location e.g. a coffee shop or other public space then you have a risk assessment to make:
  - Is the risk of “man in the middle” attack sufficient to risk using the service if you are using any personal credentials
  - You are at risk from a direct attack on the local network that you do not have at home (assuming that you can trust all of your local devices)

Email security - 1

- Email passes though an Internet based server to/from you and through potentially many other servers on its way to the addressee
  - It is NOT secure unless the content is encrypted (but that has its own problems)
- There is a mailbox account associated with each email address you use
- Mail services vary in their approach to mailbox account security
  - Most email services have been hacked at some time in the past
  - Many email addresses are known to hackers and many known email addresses are listed in the internet - https://haveibeenpwned.com/
  - Mailbox passwords need to be chosen with care and should not be used for anything else
  - Your ingoing and outgoing data is typically in plaintext and can be read on any of the servers in the chain
- Email sources can be spoofed

Email security - 2

- Email as used by a typical non-corporate user
  - Using local program client to access a Mail server provided by external provider
  - Webmail where all access is via a browser
- The Mail sever can handle inbound mail to the client in one of two ways depending on how it is configured
  - POP3
    - All new data all transferred to your computer each time the client has run
    - Historical data not accessible via web mail (can configure client to retain it for a short period)
  - IMAP
    - Data is all stored on the remote server and “mirrored” to your computer when the mail client is run
    - All data is accessible via web mail access

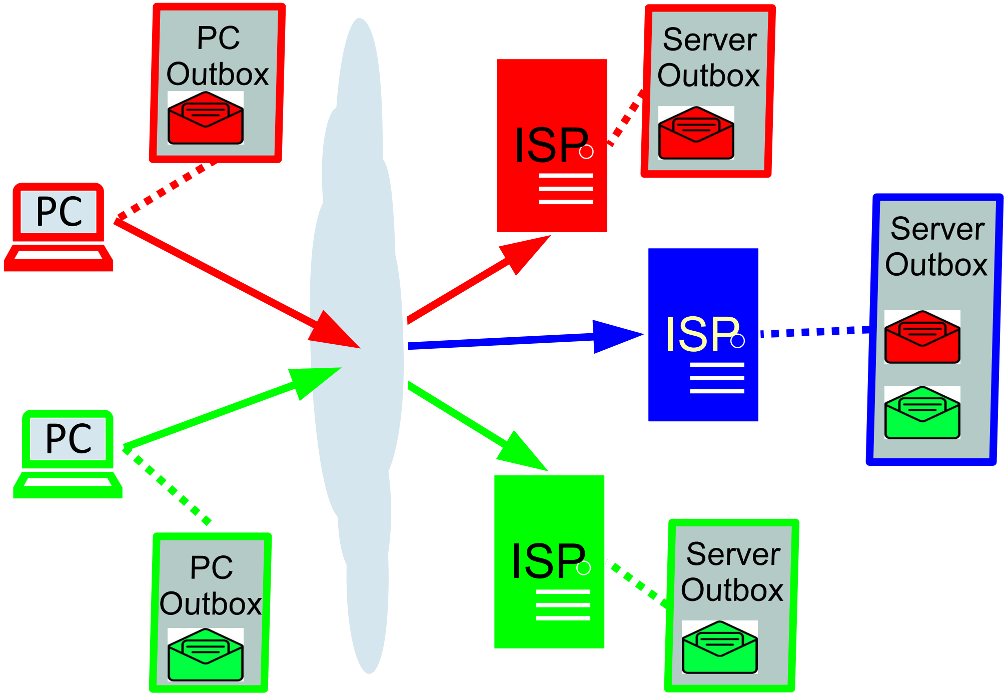
SMTP - behaviour

- Outbound email is passed through the server to its destination
  - Should not be stored persistently on the server
    - It is however worth checking occasionally as messages can sometimes be retained. When preparing this talk I found 50 messages from 4 years ago lingering there!
- Inbound email is stored on the mail server until it is read by the local mail client
  - Normally mail is deleted from the server as soon as it is transferred to the client
    - Mail client can be configured to retain it on the server for a short period
      - Useful if you need to read mail e.g. on holiday on another device e.g. a phone or by web mail. One or two weeks retention might be appropriate
    - Data retention on server is minimal and fully controllable by you
      -

IMAP behaviour

- All inbound and outbound messages are retained in the server until explicitly removed by the user
- All additional folders created in the client are retained on the server
- Benefits compared to POP3
  - Useful if you access the mailbox from multiple devices
- Issues with IMAP compared to SNMP
  - Mailboxes can grow quite large and need to be downloaded every time you connect. This can take time on a slow link. I have seen 2 Gbytes and the person was complaining his mail was slow to open!
  - Aggregation of your data might be considered a privacy risk as it is all stored on a server outside your control and even subject to different privacy legislation e.g. if located on a USA owned server
    - You do not know how often their servers are backed up and how the backup copies are handled

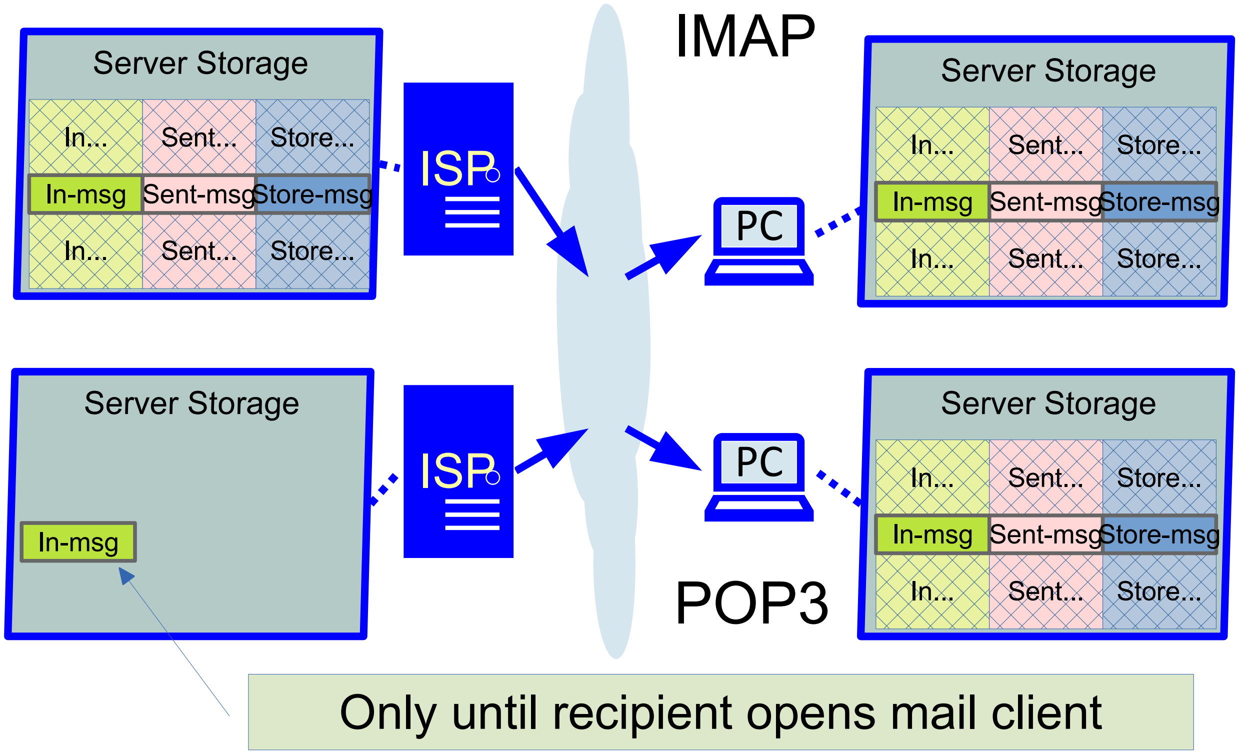
Email data flow – Sending mail



- Compose and send email from Red PC
- Goes to Red ISP Outbox
- Goes to destination Outbox
- Repeat for Green PC
- All emails finish in the outbox waiting to be collected

Icons from<a href="https://www.vecteezy.com/free-vector/email-symbol">Email Symbol Vectors by Vecteezy</a>

Email from ISP to recipient - IMAP vs POP3



Only until recipient opens mail client

- IMAP “mirrors” all Inbox, Sent Items and local storage folders with Server
- POP3 only holds messages waiting to be transferred or sent
- IMAP is good if you want to use multiple devices and see previous history
- POP3 is good if you have concerns about privacy

Cloud storage – benefits and risks

- Cloud storage is a service that is available from many source on the Internet. Some are free, others require a subscription
  - They all provide an off-site method of storing data
    - Usually this happens automatically
    - Many provide a means of sharing data between other parties
- Examples include
  - Microsoft OneDrive
  - Dropbox
  - Google Drive
  - TeamDrive

Cloud storage - benefits

- Off site backup for critical data
- Usually retains “versions” of previous copies of a file that can be retrieved
- Data can usually be shared between other parties or devices e.g.
  - Family members
  - Committee members for a club
    - Need to address GDPR issues if membership data is involved
  - Home computer and phone

Cloud Storage – points to consider

- How important is your data
  - What level of privacy do you need?
    - What sort of data do you want to store?
    - What impact will it have on YOU if it is leaked?
    - Is your cloud data stored in the EU or UK – is it protected by GDPR?
  - Is your data protected in transit to the cloud server?
    - Most is (or should be)using SSL
  - Is your data protected while stored in the cloud?
    - Most is NOT and could be accessed by provider System Administrators (or hackers)
  - Do you want to share your data with another device or person?
- Do you want a free service or are you willing to pay?

Cloud services – some options

- OneDrive – Microsoft, needs Microsoft account
  - American company, hosted on USA controlled servers
  - Encrypted in transit, probably not on server
- DropBox
  - American company, hosted on USA controlled servers
  - Encrypted in transit, probably not on server
- Google Drive
  - American company, hosted on USA controlled servers
  - Good on security, not so good on privacy
- TeamDrive
  - German company, EU hosted, GDPR compliant
  - Encrypted in transit and also securely at rest on Server
  - Recommended for personal sensitive data

Home networks

- Router can protect against inbound attacks
  - Technically protected as Network Address Translation (NAT) is required to forward the data – too complicated to go into now but a potential topic for the future!
- BUT
  - Can be configured to allow local devices to enable firewall routing through UPNP which can enable some NAT enabling a remote server to connect TO your computer (and hence your home network)
  - Default depends on ISP.
    - A recent update to my router enabled this feature without me being aware of it!